REMARKS

By this Amendment, claim 1 has been amended, claim 17 has been cancelled without prejudice and claims 18 to 71 have been added, all amendments, cancellations and/or additions merely to clarify the recited subject matter without any intention of narrowing the scope of any of the claims. Applicants have amended the currently pending claims in order to expedite prosecution and do not, by this amendment, intend to abandon subject matter of the claims as originally filed or later presented. Moreover, Applicants reserve the right to pursue such subject matter in a continuing application. Claims 1 and 18-71 are pending in this patent application. Reconsideration of the rejections in view of the remarks below is requested.

Applicants have amended the claim for benefit on the first page of the specification merely to provide a complete recitation of the parent applications to U.S. Patent Application No. US 08/786,046, applications to which benefit were claimed through the benefit claim to U.S. Patent Application No. US 08/786,046, and to update the status of U.S. Patent Application No. US 08/786,046.

The Office Action rejected claim 17 under 35 U.S.C. §112, second paragraph, as the claim refers to claims which have been cancelled by amendment. By clerical error, claim 17 was retained in this application. Applicants have cancelled claim 17 and accordingly submit that the rejection of claim 17 under 35 U.S.C. §112, second paragraph, is now moot.

The Office Action rejected claims 1 and 17 under 35 U.S.C. §103(a) as being obvious in view of U.S. Patent No. 5,224,163 ("Gasser et al.") and further in view of U.S. Patent No. 5,450,489 ("Ostrover et al."). Applicants respectfully traverse the rejection, without prejudice, for two reasons. First, the rejection with respect to cancelled claim 17 is now moot. Second, the Applicants respectfully submit that the teachings of Gasser et al. and/or Ostrover et al. fail to disclose, teach or suggest all the features recited by the claim 1.

Gasser et al. disclose a method for delegating authorization from one entity in a distributed computing system to another for a computing session wherein a session public/private encryption key pair is utilized for each computing session. The private encryption key is erased to terminate the computing session. (See, Gasser et al., col. 22, lines 28-43.) Ostrover et al. disclose a disk player that will play only authorized disks. Predetermined data blocks, including those in the lead-in section of the disk which contain content-related data, are processed to derive an authorization code. The authorization code is stored on the disk in encrypted form, using the private key of a public-key cryptosystem pair. The player processes the same disk data to derive a computed code; the player also uses the

paired public key to decrypt the encrypted authorization code on the disk. Play of the disk ensues only if the decrypted authorization code matches the computed code. The same technique can be used to control not play of the disk as a whole, but play in certain specific modes. (See, Ostrover et al., col. 2, lines 41-56.)

The Office Action asserted that the combination of Gasser et al. and Ostrover et al. suggests or teaches all the features of claim 1. However, Applicants' respectfully submit that Gasser et al. and/or Ostrover et al. fail to at least disclose, teach or suggest a method which, among other things, denies access to a certifying authority's public key used to verify a digital signature of the certifying authority, provides a recipient with a message containing a rule regarding maintaining secrecy of the public key, digitally signs the message by which the recipient agrees to the rule, and permits the recipient to utilize the public key in response to the digital signing, as generally recited in independent claim 1.

Applicants submit that Gasser et al. provide no disclosure, teaching or suggestion regarding denying access to a certifying authority's public key. Rather, Gasser et al. disclose that users know the public keys of certifying authorities and appear to have ready access to them through the naming service. (See, e.g., col. 7, lines 29-35, col. 8, line 19-51 of Gasser et al.) Moreover, as acknowledged by the Office Action, Gasser et al. provide no disclosure, teaching or suggestion regarding providing a recipient with a message containing a rule regarding maintaining secrecy of the certifying authority's public key, digitally signing the message by which the recipient agrees to the rule, and permitting the recipient to utilize the public key in response to the digital signing.

Ostrover et al. do not overcome any of the deficiencies of Gasser et al. nor independently disclose, teach or suggest the features of claim 1. Firstly, Ostrover et al. provide no disclosure, teaching or suggestion regarding a certifying authority's public key. Only basic public key cryptography is discussed by Ostrover et al. Further, Ostrover et al. provide no disclosure, teaching or suggestion regarding denying access to a public key. Indeed, Ostrover et al. promote that the public key may be generally available (see, e.g., col. 3, lines 23-26 and lines 39-44, of Ostrover et al.) without causing compromise of their systems. Of course, disclosure of and general access to the private key is a very different matter. Finally, Ostrover et al. provide no disclosure, teaching or suggestion regarding providing a recipient with a message containing a rule regarding maintaining secrecy of the certifying authority's public key, digitally signing the message by which the recipient agrees to the rule, and permitting the recipient to utilize the public key in response to the digital

signing. Ostrover et al. simply do not disclose, teach or suggest a method to permit utilization of a public key in response to digitally signing of a message that contains a rule regarding maintaining secrecy of the public key.

Therefore, for at least the above reasons, Gasser et al. and/or Ostrover et al. fail to disclose, teach or suggest all the features recited by claim 1. As a result, Applicants respectfully submit that the rejection under 35 U.S.C. §103(a) should be withdrawn and the claims allowed.

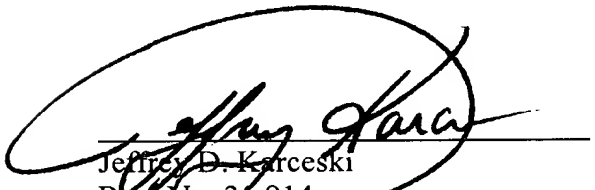
Further, Applicants respectfully submit that new independent claim 22 is patentable over the prior art of record at least because the prior art of record fails to disclose, teach or suggest a method for processing a commercial transaction employing cryptography to enforce a policy per transaction that is encoded at least in part as an attribute, comprising receiving, from a participant to a commercial transaction, a cryptographically authorized attribute approved by a sponsor, checking the attribute presented to determine if the transaction may be processed and meet a requirement of the policy the attribute represents, checking that the sponsor is valid in order that the transaction may be processed, and determining to allow the transaction to be processed based upon the checking of the attribute and of the sponsor. Further, Applicants respectfully submit that new independent claim 39 is patentable over the prior art of record at least because the prior art of record fails to disclose, teach or suggest a method for processing a commercial transaction employing cryptography to enforce a policy per transaction that is encoded at least in part as an attribute, comprising presenting, by a participant to a commercial transaction, a cryptographically authorized attribute as approved by a sponsor, the attribute representing a requirement of the policy and the recipient of the attribute to determine from the attribute if the transaction may be processed and meet the requirement and to check that the sponsor is valid in order that the transaction may be processed. Applicants also respectfully submit that new independent claim 52 is patentable over the prior art of record at least because the prior art of record fails to disclose, teach or suggest an electronic system for processing of commercial transactions according to a policy, comprising computer program code configured to receive, from a participant to a commercial transaction, transaction content and a cryptographically authorized attribute as approved by a sponsor, computer program code configured to check the transaction content and the cryptographically authorized attribute to determine if the transaction may be processed and meet a requirement of the policy the attribute represents, and computer program code configured to determine to allow the transaction to be processed based upon the check of the transaction content and the attribute. Finally, Applicants also respectfully submit that new

independent claim 68 is patentable over the prior art of record at least because the prior art of record fails to disclose, teach or suggest a method for processing a commercial transaction employing cryptography to enforce a policy per transaction that is encoded at least in part as an attribute, comprising approving by a sponsor a cryptographically authorized attribute to be used by a participant to a commercial transaction, the attribute representing a requirement of the policy and a recipient of the attribute to determine from the attribute if the transaction may be processed and meet the requirement and to check that the sponsor is valid in order that the transaction may be processed. The remaining claims, which depend from these independent claims are believed to be patentable at least for these reasons and also for the additional reasons recited thereby.

All objections and rejections having been addressed, it is respectfully submitted that the present application is in condition for allowance. If questions relating to patentability remain, the Examiner is invited to contact the undersigned to discuss them.

Should any fees be due, please charge them to our deposit account no. 03-3975, under our order no. 061047/0264493. The Commissioner for Patents is also authorized to credit any over payments to the above-referenced deposit account.

Respectfully submitted,
PILLSBURY WINTHROP LLP



Jeffrey D. Karceski
Reg. No. 35,914
Tel. No. 703-905-2094
Fax No. 703-905-2500

JDK/JGH
P. O. Box 10500
McLean, VA 22102
(703) 905-2000